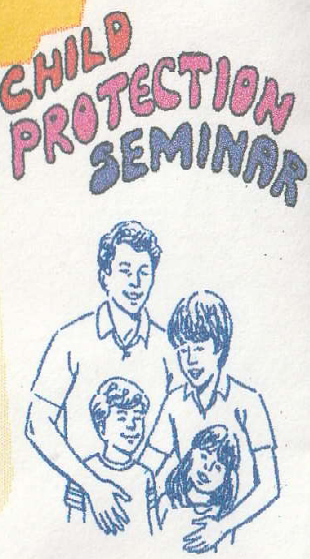
Keeping Kids Safe

Internet tips & Tools for Parents & Teachers



Lionel Hartley

Keeping Kids Safe
(Multimedia)
Internet Tips & Tools for Parents & Teachers
Lionel Hartley
Copyright ©2000 Lionel Hartley
Published by Salubrity™ Seminars
All rights reserved in all countries.
No part of this digital book may be used or reproduced in any manner whatsoever without written permission except in the case of brief quotations embodied in critical articles and reviews.
Typeset in Times using a 512 MAC-Plus and Aldus PageMaker
Illustrated with original drawings by Lionel Hartley

Contents

Chapter 1 – The Basics 4

Chapter 2 - Setting Age-Appropriate Rules 11

Chapter 3 - Respectful Online Behaviour 17

Chapter 4 – Password Habits 24

Chapter 5 – Privacy Settings and Parental Controls 31

Chapter 6: Software Helpers 36

Chapter 1 – The Basics

Helping children use the Internet safely is a mix of setting clear expectations, using available safety tools, and keeping communication open.E

Here are the very basic practical tips for parents (& Teachers):

1. Talk About Online Safety Early

Explain that not everyone online is who he or she claims to be.

Encourage children to tell you if they see something upsetting or if someone makes them uncomfortable.

Keep conversations ongoing rather than having just one “internet safety talk.”

2. Set Age-Appropriate Rules

Consider agreeing on:

Which websites, bulletin boards and games are allowed.

How much screen time is appropriate.

Whether devices can be used in bedrooms or only in shared spaces.

Rules about downloading apps or making online purchases.

3. Protect Personal Information

Teach children never to share:

Full name (when unnecessary)

Home address

School name

Phone number

Passwords

Photos or videos that reveal personal details

4. Use Privacy and Parental Controls

Enable parental controls on devices and browsers.

Review privacy settings on any accounts.

Keep devices updated with the latest security patches.

In the future there will be special programs to assist with this (these are still (in y2000) under development).

5. Teach Critical Thinking

Help children learn to:

Question information they see online.

Recognize scams, phishing attempts, and fake giveaways.

Avoid clicking suspicious links or downloading unknown files.

6. Encourage Respectful Online Behaviour

Discuss:

Being kind and respectful online.

That anything shared online may be difficult to remove completely.

7. Know Who They're Talking To

Be aware of your child's online friends and bulletin board contacts.

Remind children never to meet someone they've only found about online without a trusted adult present.

8. Watch for Warning Signs

Pay attention if your child:

Becomes secretive about computer activities.

Seems anxious or upset after screen time.

Suddenly avoids school or friends.

Receives bulletin board messages from unfamiliar

people.

These signs don't necessarily indicate a problem, but they can be a reason to start a conversation.

9. Create Strong Password Habits

Use unique, strong passwords for important accounts.

Teach children never to share passwords with friends.

10. Be a Positive Role Model

Children often copy adults' computer habits. Consider:

Demonstrating balanced screen use.

Respecting privacy online.

Showing how to verify information before sharing it.

Model how you keep your own relationships safe. (For example, I have my computer set up in the family room and anyone in the family can peer over my shoulder anytime to see what I am looking at, who I am emailing, and what I am writing.)

11) If Something Goes Wrong

If your child experiences inappropriate contact, or sees harmful content:

Stay calm and listen.

Save evidence (screenshots or messages).

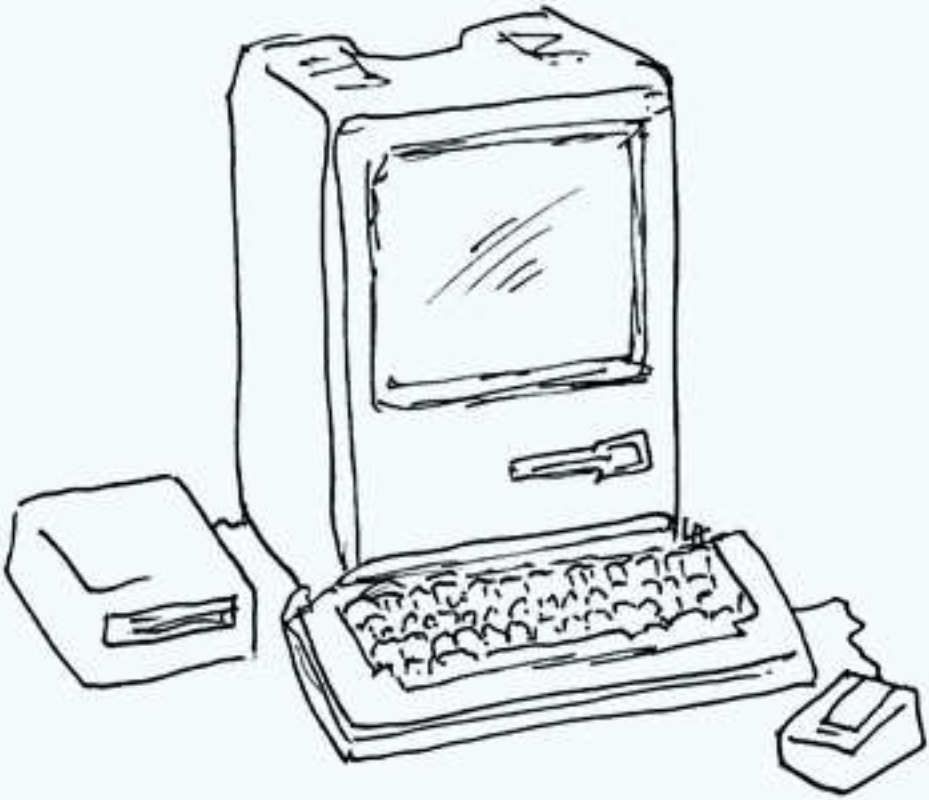
Block and report the person or their content.

Change passwords if needed.

Contact the school or internet service provider if appropriate.

Report serious incidents to local authorities if there are threats, exploitation, or other criminal behaviour.

The most effective online safety strategy is combining technology (such as parental controls) with trust and regular conversations. Children who feel comfortable talking to their parents are more likely to seek help when they encounter problems online.



Keeping Kids Safe [p10] Lionel Hartley

Chapter 2 - Setting Age-Appropriate Rules

Setting age-appropriate Internet rules works best when the expectations are clear, consistent, and matched to your child's maturity. As children grow, rules can become more flexible while still emphasizing safety.

a) For children ages 5–8

Focus on supervision and simple boundaries.

Rules might include:

* Only use approved programs, websites, and games.
* Ask a parent before downloading anything.
* Use devices in shared family spaces.
* Tell an adult if something online is confusing, scary, or upsetting.
* Never communicate with strangers online.

b) For children ages 9–12

Introduce more independence while maintaining oversight.

Rules might include:

* Only communicate with people you know in real life, unless a parent has approved otherwise.
* Never share personal information such as your address, school, or phone number.
* Ask permission before making purchases or installing new programs.
* Follow agreed screen-time limits.
* Be respectful in correspondence.

c) For teenagers (13+)

Encourage responsibility and open communication.

Rules might include:

* Think before putting anything online; assume anything shared could become public.
* Protect passwords.

* Be cautious when interacting with new online contacts or bulletin board posters.

* Balance online activities with school, sleep, exercise, and family time.

* Talk to a trusted adult if you experience bullying, harassment, or pressure online.

d) Creating Family Internet Rules

i) Create rules together.

Involving children in setting expectations helps them understand the reasons behind the rules.

ii) Explain the “why.”

For example, “We don’t share our location because it helps keep you safe.”

iii) Be consistent.

Apply rules fairly and follow through with agreed consequences if they’re broken.

iv) Review regularly.

As your child gets older or starts using new programs or devices, update the rules together.

v) Lead by example.

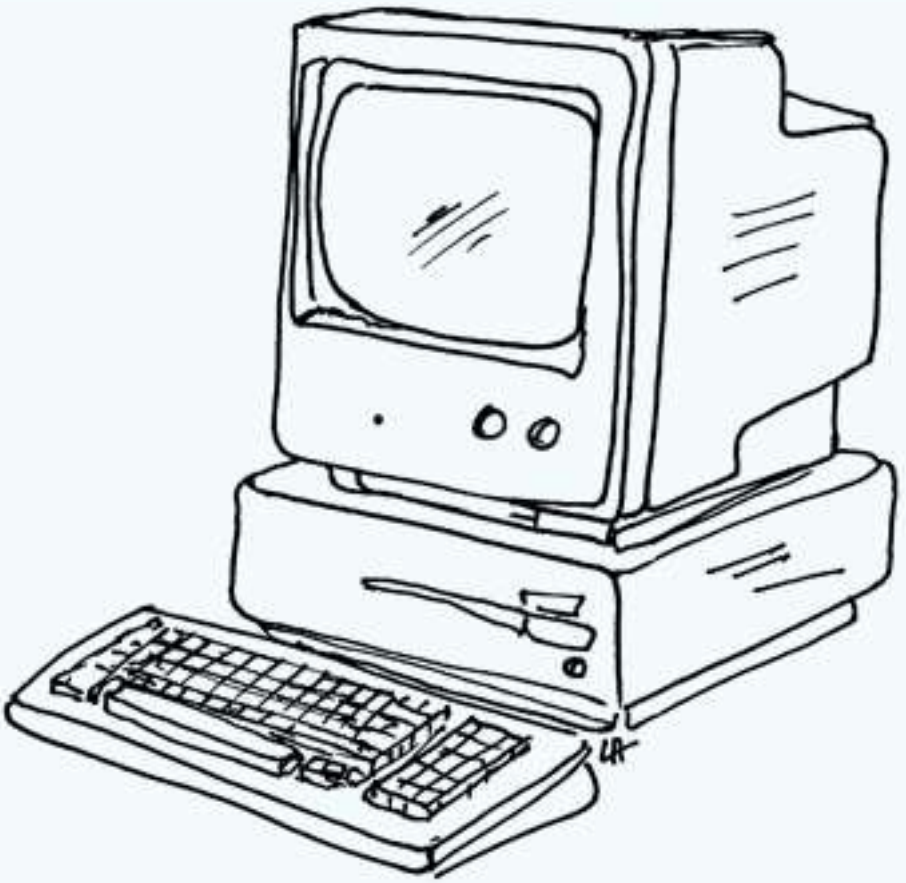
Demonstrate healthy screen habits, respectful online behaviour, and responsible use of technology.

vi) Sample Family Internet Agreement

* I will be kind and respectful online.
* I will not share personal information without asking a parent or caregiver.
* I will only use programs and games that my parent or caregiver has approved.
* I will tell a trusted adult if something online makes me uncomfortable.
* I will ask before downloading programs or making purchases.

* I will follow our agreed screen-time limits.
* I will keep my passwords private (except from my parent or caregiver if that is our family rule).
* I will balance screen time with homework, physical activity, and family time.

By keeping rules simple, age-appropriate, and regularly discussing them as a family, parents can help children build safe and responsible online habits that will serve them well as they grow.



Keeping Kids Safe [p16] Lionel Hartley

Chapter 3 - Respectful Online Behaviour

Encouraging respectful online behaviour starts with helping children understand that the same values they use in person—kindness, honesty, and respect—also apply online.

Ways to Encourage Respectful Online Behaviour

1. Teach the "Think Before You Share" Rule

Encourage children to ask themselves:

* Is it true?
* Is it kind?
* Is it necessary?
* Would I be comfortable if my family, teacher, or future employer saw this?

If the answer is "no," it's better not to write it.

2. Model Positive Digital Behaviour

Children learn by watching adults. Show them how to:

* Communicate politely online.
* Respect other people's opinions.
* Avoid emailing when angry or frustrated.
* Credit others when sharing their work.

3. Discuss Digital Footprints

Explain that:

* Photos, comments, and messages can remain online for a long time.
* Even deleted content may have already been copied or shared.
* A positive digital footprint can benefit future education and career opportunities.

4. Promote Empathy

Ask children to consider:

* “How would you feel if someone sent this email message to you?”
* “Could this comment hurt someone’s feelings?”
* “What would be a kinder way to say this?”

Helping children think from another person’s perspective builds empathy and reduces hurtful behaviour.

5. Talk About Online Bullying

Help children understand that online bullying includes:
* Sending mean or threatening messages.
* Excluding others on purpose.
* Sharing embarrassing photos or rumours.
* Pretending to be someone else to hurt another person.

Encourage them to:
* Never join in.
* Support friends who are being bullied.
* Tell a trusted adult if they witness or experience

bullying.

6. Encourage Respect for Privacy

Teach children to:

* Ask permission before emailing photos or videos of others.
* Keep personal conversations private.
* Respect other people's boundaries online.

7. Teach Responsible Communication

Remind children that online messages can be misunderstood because they lack facial expressions and tone of voice. Encourage them to:

* Use respectful language.
* Avoid typing messages when they are upset or angry.
* Pause and pray before responding to upsetting comments.

8. Praise Positive Online Choices

Recognize when children:
* Show kindness online.
* Help someone who is struggling.
* Report inappropriate behaviour.
* Make thoughtful decisions about what they share.

Positive reinforcement encourages these behaviours to continue.

9) Family Conversation Starters

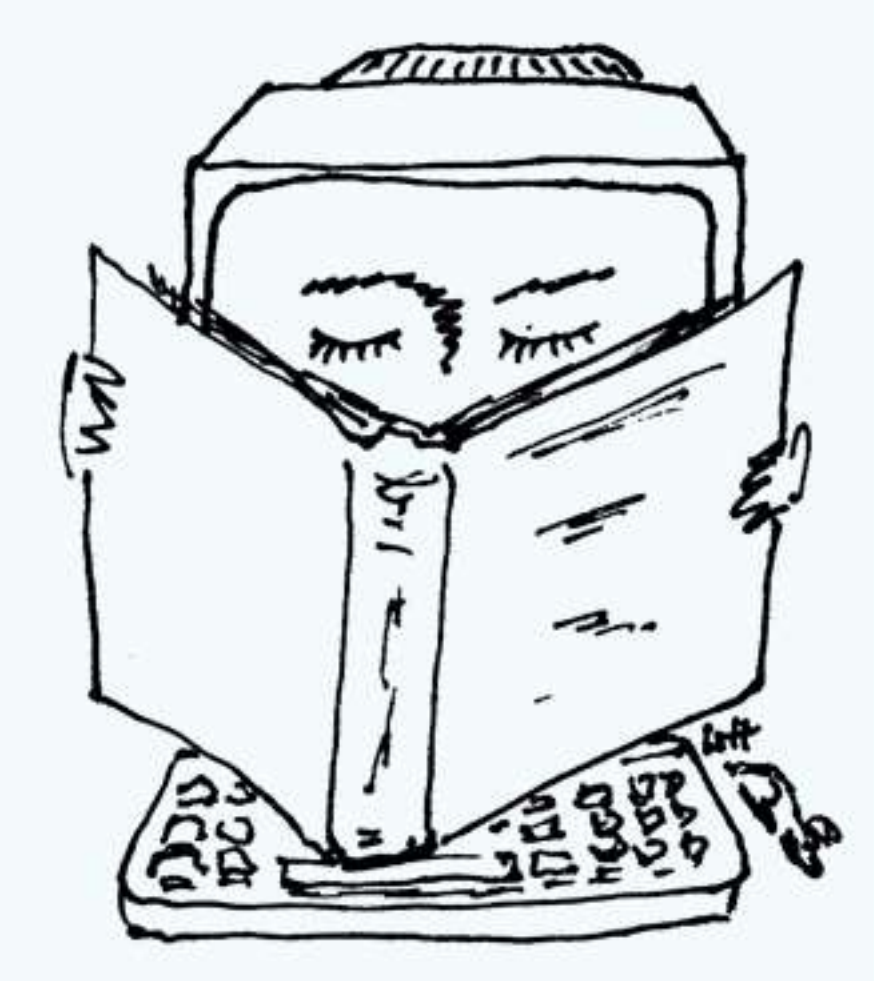
Use everyday situations to discuss online behaviour:
* “What would you do if you know someone is being bullied online?”
* “How can you disagree with someone respectfully?”
* “What makes someone a good email friend?”
* “What would you do if a friend asked you to keep an online secret that made you uncomfortable?”

10) Family Online Respect Pledge

You could create a simple family agreement such as

* We treat others online with kindness and respect.
* We think before we email, comment, or share.
* We protect our own privacy and respect other people's privacy.
* We do not participate in bullying or gossip.
* We tell a trusted adult if we see or experience harmful behaviour online.
* We use technology to learn, connect, and make a positive difference.

By reinforcing these habits through regular conversations and positive role modelling, parents can help children become responsible, respectful, and confident digital citizens.



Keeping Kids Safe [p23] Lionel Hartley

Chapter 4 – Password Habits

Creating strong password habits is one of the simplest and most effective ways to protect your child's email accounts. The goal is to help children understand that passwords are like the keys to their Internet lives and should be treated with care.

Tips for Building Strong Password Habits

1. Create Strong, Unique Passwords

Teach children to use passwords that are:

* At least 12–16 characters long.
* A mix of uppercase and lowercase letters, numbers, and symbols (when allowed).
* Different password for every account.

Avoid using:

* Names or birthdays.

* Pet names.
* Favourite sports teams.
* Simple patterns like “123456” or “password.”

2. Use Easy-to-Remember Pass-phrases

Instead of a single word, encourage a pass-phrase made up of several unrelated words.

For example:

* AnnatheCowLoves2email

These are generally easier to remember and harder for others to guess.

3. Never Share Passwords

Teach children that passwords should only be shared with a trusted parent or caregiver if that is part of your family’s rules. Explain that even close friends should not know their passwords.

Remember:

If you have a friend
Then keep them so.
Let not your friend
Your secrets know
For if your friend becomes your foe
Then all the world will your secrets know!

4. Use a Password Manager Program

As children get older, consider using a reputable password manager Program to:

* Generate strong passwords.
* Store passwords securely.
* Reduce the need to remember multiple complex passwords.

5. Watch Out for Scams

Teach children never to enter their password after

clicking on links in unexpected emails or bulletin boards. Encourage them to ask an adult if they are unsure whether a message is genuine.

6. Keep Passwords Private

Remind children:

* Never write passwords where others can easily find them.
* Don’t save passwords on a shared or public (e.g. library or school) computers.
* Always log out of shared devices.

7. Update Passwords When Needed

Change passwords immediately if:

* An email account may have been hacked or accessed without authorisation.
* A password has been shared accidentally.
* A website or service reports a security breach.

8) Fun Ways to Teach Password Safety

i) The Secret Key Analogy:

Explain that a password is like the key to their bedroom or personal diary—only trusted people should have access.

ii) Password Challenge:

Have children create a strong pass-phrase and discuss why it is more secure than a short, simple password.

iii) Spot the Strong Password:

Compare examples together and ask which is safer:

* Rosemary123
* Never_share4ever!

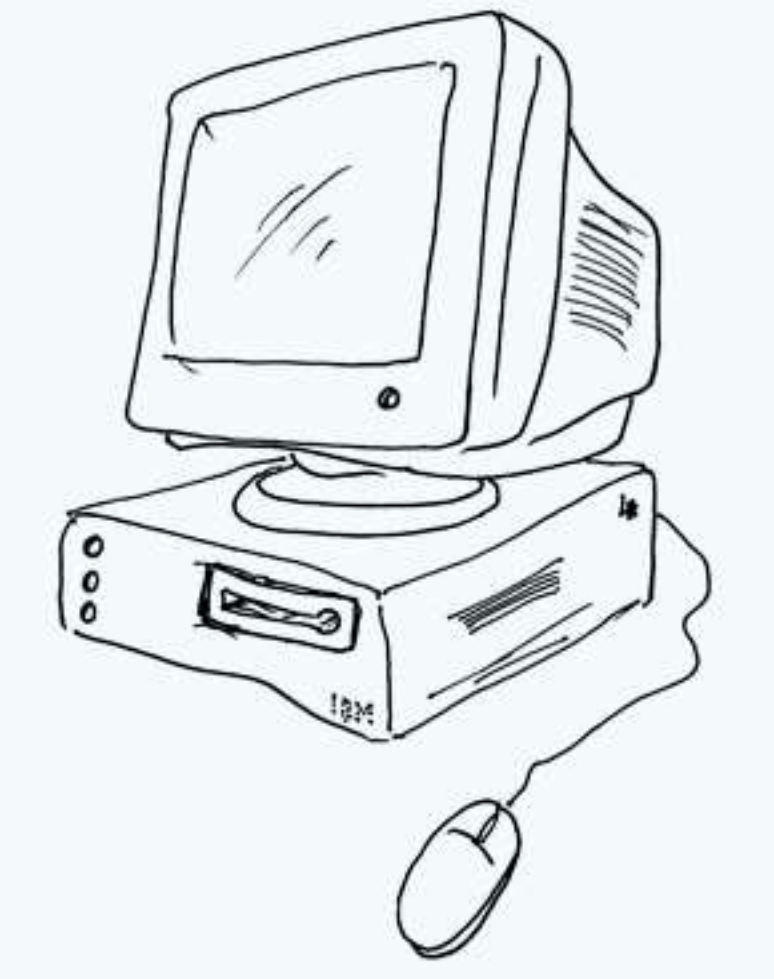
9) Family Password Rules

Consider creating a simple family agreement:

* We use a different password for every important account.

* We create long, unique passwords or pass-phrases.
* We never share passwords with friends.
* We tell a parent or caregiver immediately if we think an account has been compromised.

By making password safety part of everyday digital habits, children can develop the skills they need to protect their personal information and confidently navigate the online world.



Keeping Kids Safe [p30] Lionel Hartley

Chapter 5 – Privacy Settings and Parental Controls

Privacy settings and parental controls are valuable tools that can help create a safer online experience for children. While they don't replace supervision and open conversations, they can reduce exposure to inappropriate content and help parents manage their child's online activities.

a) Privacy Settings

Privacy settings control who can see your child's information and interact with them online. Review these settings together whenever your child starts using a new program or device.

i) Limit Personal Information

Help your child avoid sharing

* Full name
* Home address
* Phone number
* School name
* Date of birth (if not required)

ii) Manage Location Sharing

* Turn off location sharing unless it is needed.
* Check which programs have permission to access your child's location.
* Explain why sharing their location with strangers can be risky.

iii) Control Communication

Many programs or applications allow you to:

* Approve who can contact your child.
* Restrict direct messages.
* Filter unwanted messages.
* Block or report users who behave inappropriately.

b) Parental Controls

Parental controls help parents guide and monitor how children use technology. Most devices and online services include built-in tools.

i) Screen Time Limits

Set daily limits for:

* Entertainment programs
* Computer Games
* Email time
* Overall device use

Scheduling “screen-free” times—such as during meals, homework, and bedtime—can help encourage healthy routines.

ii) Content Filters

Use filters to:

* Block inappropriate websites.
* Restrict explicit music, games or video clips.
* Filter search results.
* Limit age-inappropriate videos and programs.

iii) Purchase Controls
Protect against accidental spending by:
* Requiring a password or approval for purchases.
* Disabling in-program purchases if appropriate.
* Reviewing subscriptions regularly.

iv) Activity Reports
Many parental control tools provide reports showing:
* Screen time
* Programs used
* Websites visited
* Time spent on different activities

These reports can help start conversations about

healthy technology use rather than being used solely for monitoring.

v) Tips for Using Parental Controls Effectively

* Explain to your child why the controls are being used—they are there to support safety, not to punish.
* Adjust settings as your child matures and demonstrates responsible online behaviour.
* Review privacy and safety settings regularly, as some programs often update their features.
* Balance technology tools with regular conversations about online safety and responsible digital citizenship.

Privacy settings and parental controls are helpful safeguards, but they work best alongside trust, guidance, and ongoing communication. Children who understand why these protections are in place are more likely to make safe and responsible choices, even when adults are not present.

Chapter 6: Software Helpers

Although as we rapidly move into the future other tools will no doubt be developed, at present we must rely on keyword-filtering and site-blocking software the primary tools for parental control.

1) Dedicated Monitoring Software

i) **Net Nanny**: Filters text in real-time across web browsers, chat rooms (like IRC), and emails, masking profanity and blocking flagged imagery.

ii) **CyberPatrol**: A heavily utilized corporate and home filter that relieson a regularly updated blacklist database of "cyber-not-cents" URLs, categorized into topics like violence, pornography, and gambling.

iii) **CYBERsitter**: Known for its strict phrase-filtering

capabilities, this software blocks access to websites if they contain specific adult keywords and can secretly log a teenager's online activity for parental review.

iv) **SurfWatch**: Interceptsdata traffic and blocks specific URLs and newsgroups based on a proprietary database.

2) ISP-Built Controls

America Online (AOL) Parental Controls featur robust, built-in "Kids Only" and "Young Teen" account settings that lock users into a heavily curated walled garden, blocking external web surfing and restricting instant messaging.

3) Operating System & Browser Features

Microsoft Internet Explorer 5.0 Content Advisor is built directly into this web browser. This tool allows parents to use the RSACi (Recreational Software Advisory

Council on the Internet) rating system to block sites based on levels of language, nudity, sex, and violence.

Living
Life to
Salubrify™
Seminars
the Full